Report: 03 May 2024

Queensland Department of Transport and Main Roads

FOR PUBLICATION

PRIVACY IMPACT ASSESSMENT: MOBILE PHONE AND SEATBELT TECHNOLOGY PROGRAM 2023

IIS Partners
INFORMATION INTEGRITY SOLUTIONS

Contents

1. Executive summary 1
   - 1.1 IIS's overall view 1
   - 1.2 Recommendations and best practice suggestions 2
2. About the PIA 5
3. Project description 6
   - 3.1 Background 6
   - 3.2 Project objectives and scope 6
   - 3.3 Project status 7
   - 3.4 Program stakeholders 7
     - 3.4.1 QRO 7
     - 3.4.2 TMR 7
     - 3.4.3 IAP Supplier 7
     - 3.4.4 Camera and AI provider 8
     - 3.4.5 Community stakeholders 8
   - 3.5 Legislative framework 8
     - 3.5.1 Transport Operations (Road Use Management) Act 1995 8
     - 3.5.2 State Penalties Enforcement Act 1999 10
     - 3.5.3 Information Privacy Act 2009 10
   - 3.6 System and data components 11
     - 3.6.1 Transport Registration and Integrated Licensing System (TRAILS) / Transport Integrated Customer Access (TICA) 11
     - 3.6.2 MPST Incident Adjudication Portal (IAP) 11
     - 3.6.3 Customer-facing Online Services 12
     - 3.6.4 Camera and print batching 12
   - 3.7 Nature of information and information flows 12
     - 3.7.1 Nature of information 12
     - 3.7.2 Information flow 13

4. Approach to risk analysis 15
4.1 Inherent privacy risks 15
4.2 Positive privacy aspects 16
4.3 Residual privacy risk level 16
5. Findings and recommendations 17
5.1 Review of 2022 PIA Report 17
5.2 Business processes, practices, polices, and organisational aspects 23
5.2.1 Changes to the MPST adjudication process 23
5.2.2 MPST Unit's move to QRO 26
5.2.3 Design of personal information handling practices 30
5.2.4 Privacy complaints management process 37
5.3 System (technical) components and data 38
5.3.1 Functional and technical changes to the existing IAP 38
5.3.2 New IAP for QRO with external Supplier 39
5.3.3 Changes to camera scheduling 45
5.4 Other issues 46
5.4.1 Media attention and public expectations 46
5.5 Conclusion 48
6. Appendix A – Scope and methodology 49
7. Appendix B – Assessment against the IPPs 50

Glossary

Abbreviation or term	Expansion or definition
AI	Artificial intelligence
APPs	Australian Privacy Principles in the Privacy Act 1988 (Cth).
BAU	Business as Usual
CDOP	Camera Detected Offence Program
IAP	Incident Adjudication Portal
IIS	Information Integrity Solutions Pty Ltd
IP Act	*Information Privacy Act 2009*
IPOLA Act	*Information Privacy and Other Legislation Amendment Act 2023*
IPPs	Information Privacy Principles in the IP Act
KPIs	Key performance indicators
MoG	Machinery of Government
MOU	Memorandum of Understanding
MPST	Mobile Phone and Seatbelt Technology
PIA	Privacy Impact Assessment
QGCDG	Queensland Government Customer and Digital Group
QRO	Queensland Revenue Office
QT	Queensland Treasury
RTI	Right to Information. Queensland has a framework for giving the community access to information held by the Government, under the *Right to Information Act 2009* and the IP Act.

Abbreviation or term	Expansion or definition
SCO	Service Centre Online
SPE Act	*State Penalties Enforcement Act 1999*
SPER	State Penalties Enforcement Registry
TICA	Transport Integrated Customer Access
TMR	Department of Transport and Main Roads
TORUM Act	*Transport Operations (Road Use Management) Act 1995*
TRAILS	Transport Registration and Integrated Licensing System
UX	User experience

1. Executive summary

The Queensland Department of Transport and Main Roads (TMR), in collaboration with the Queensland Revenue Office (QRO), has asked IIS Partners (IIS) to conduct a Privacy Impact Assessment (PIA) on the Mobile Phone Seatbelt Technology cameras (MPST) program.

IIS conducted the original PIA on the implementation of the MPST project, with the final PIA report being delivered in February 2022. One of the recommendations from the original PIA was to undertake a review within a year and to conduct a further PIA to demonstrate ongoing privacy best practice and to assess privacy risks arising from the changes to the MPST project.

Since the original PIA, many changes have occurred and are being anticipated. These include the MPST Unit moving to QRO, changes to the MPST adjudication process, the process to implement a new Incident Adjudication Portal (IAP) solution, and further business and technical changes.

This report:

- Maps information flows based on current arrangements, taking into account the MPST Unit's move from TMR to QRO
- Identifies privacy risks and issues arising from the MPST program and the proposed new processes and systems, as assessed against the Information Privacy Principles (IPPs) in the *Information Privacy Act 2009* (Qld) (IPA Act), regulator guidance and privacy best practice
- Makes recommendations to address identified risks and ensure privacy and security compliance, as well as best practice suggestions for improving privacy practice.

The scope and methodology for the PIA are set out in Appendix A.

1.1 IIS's overall view

IIS has not identified any show-stopping privacy issues for the MPST program, and we consider that its business as usual (BAU) operations are largely compliant with the IPPs – see Appendix B for a high-level assessment.

As with the original PIA, the MPST program has a high degree of inherent privacy risk due to its nature as a form of surveillance that captures potentially sensitive images across a broad range of the Queensland population as well as interstate drivers. On the other hand, there are a number of positive privacy aspects that mitigate the inherent privacy risk:

- The program continues to maintain the protections outlined in the 2022 PIA, for example:
  - The collection and use of images is authorised by law
  - Images are deleted quickly from cameras and from the camera and AI provider's systems, once an offence is ruled out

- Decisions about offences are not automated, but validated by multiple points of human review
- The camera and AI provider continues to improve the accuracy and consistency of AI image decision-making
- Access to the IAP is subject to a range of organisational and technical controls
- The MPST Unit has been operational for approximately two years, and has developed ways of working to appropriately handle the information that it collects
- There is widespread recognition among QRO program management and leadership of the importance of privacy.

Overall, the MPST program has been operating smoothly in BAU, albeit with some negative media attention, which is further discussed in the report. IIS considers that the key privacy risk to be mitigated can be described as: **Unauthorised access to or misuse of TMR and QRO information by staff, contractors or third parties resulting in non-compliance with the law, harm to the customer, reputational damage to government and eroded public trust**.

Based on review of documentation and discussions with relevant stakeholders, we consider that more can be done in the following areas to reduce this risk:

- From a business processes, practices, polices, and organisational perspective – strengthen privacy governance within QRO and MPST Unit:
  - Further access controls and audit practices
  - Strengthened retention and deletion practices for images and personal information
  - Better documentation of policies, standards and procedures, with accompanying training
- From a technical perspective – conduct further privacy risk due diligence for the new IAP:
  - Perform a privacy threat analysis and strengthen mechanisms to prevent, detect and respond to unauthorised access to and misuse of camera images.

1.2 Recommendations and best practice suggestions

Where IIS has identified a risk to be mitigated (including, but not limited to, non-compliance with the IPPs), we provide a **recommendation**. Where we have identified an area for improvement, we provide a **suggestion** for best practice.

IIS has made eight recommendations to address privacy risks identified by the PIA, especially those that may lead to unauthorised access to or misuse of TMR information and therefore breach IPP 4 (Storage and security), IPP 9 (Use of personal information only for relevant purposes), IPP 10 (Limits on use) and/or IPP 11 (Limits on disclosure).

IIS provided a draft version of the report to TMR and QRO for their review. Based on their feedback, we updated our findings and recommendations to reflect factual matters and adjusted some of the timelines, to ensure that they can be readily implemented.

Recommendation	Who	Timeframe
Recommendation 1 – Explore more granular access settings for MPST Unit staff, as part of new IAP	QRO and IAP supplier	Before go-live of new IAP
Recommendation 2 – Review and update formal audit policy and procedure for the IAP	QRO	Within 6 months
Recommendation 3 – Review and update formal policy for retention and deletion of camera images	QRO	Within 6 months
Recommendation 4 – Review and update email archive/retention policy	QRO	Within 6 months
Recommendation 5 – Explore feature for flagging and restricting access to sensitive images in the new IAP	QRO and IAP supplier	As part of subsequent releases following go-live of the new IAP
Recommendation 6 – Develop formalised processes and procedures that cover the MPST Unit's workflow lifecycle, as prioritised using a risk-based approach	QRO	Within 6 months, to be revisited when significant changes occur
Recommendation 7 – Review and update specific information handling, privacy and security training content as part of MPST induction	QRO	Within 6 months, to be revisited when significant changes occur
Recommendation 8 – Perform a privacy threat analysis and strengthen mechanisms to prevent, detect and respond to unauthorised access to and misuse of camera images	TMR, QRO and relevant contracted party	Within 6 months and ongoing

We have made an additional seven best practice suggestions that go beyond compliance.

Best practice suggestions	Who	Timeframe
Suggestion 1 – Review and update existing procedures and implement updated policies, while fostering working relationship for responding to MPST privacy and security incidents and breaches	TMR, QRO and QT	Within 6 months and ongoing
Suggestion 2 – Review Correspondence Guide to address current issues and gaps in handling customer complaints and enquiries to the MPST Unit	TMR and QRO	Within 6 months
Suggestion 3 – Consider privacy best practices for data migration	TMR, QRO and IAP supplier	Before go-live of new IAP
Suggestion 4 – Consider avoid storing personal details in the new IAP	TMR, QRO and IAP supplier	Before go-live of new IAP
Suggestion 5 – Formalise privacy testing process	TMR and QRO	Before go-live of new IAP
Suggestion 6 – Confirm the monitoring approach for the operating model for the new IAP	TMR and QRO	Before go-live of new IAP
Suggestion 7 – Revisit and document decision as to whether the image pixelation feature should be used by the MPST Unit	QRO	Within 6 months

2. About the PIA

TMR, in collaboration with QRO, engaged IIS to:

- Address the following in scope matters pertaining to the MPST program:
  - Review the original privacy impact assessment (PIA) to consider remediation of privacy risks identified and implementation of recommendations
  - Support TMR in delivering the business objectives of the PIA including processes, practices, policies, and organisational aspects
  - Support TMR in delivering the technical objectives of the PIA including system and technical components and data aspects
- Identify the privacy and security risks associated with the above and provide recommendations to mitigate such risks.

This PIA builds upon an earlier PIA IIS conducted for the MPST program which was issued in February 2022.

How to read this PIA report:

- Section 3 of the report is descriptive and provides contextual information on the MPST program, including
  - System components
  - The personal information that will be handled
  - The proposed personal information flows.
- Section 4 provides an overview of IIS's approach to the privacy risk assessment and our assessment of the MPST program's inherent privacy risks.
- Section 5 set out IIS's analysis, findings, recommendations and suggestions.
- The scope and methodology for the PIA are set out in Appendix A.

3. Project description

3.1 Background

TMR is working with QRO to manage the MPST program. TMR operates the mobile phone and seatbelt detection cameras (the cameras), which were rolled out in July 2021. The MPST Unit undertakes the infringement processing using a TMR-developed web-based IAP. Issuing of infringement warning letters started in July 2021 for an initial period of three months and enforcement of mobile phones and seatbelt offences started in November 2021. Where offences are determined, an infringement notice is generated by the IAP system and sent to the contracted mailing house for printing and distribution.

IIS conducted the original PIA on the MPST program, with the final PIA report being delivered in February 2022. The original PIA recommended that TMR undertake a review within a year of the extent to which recommendations had been implemented, and to conduct a further PIA to a) demonstrate ongoing privacy best practice and b) assess privacy risks arising from any changes to the MPST program.

Since the original PIA, Queensland Treasury (QT) initiated the Fines Modernisation Program (FMP) which aimed to develop a single integrated approach to fine and penalty debt administration within QRO. This resulted in a Machinery of Government (MoG) change and the transition of the MPST Unit from TMR to QRO. As part of this transition, a new IAP needed to be developed in order to 'decouple' the platform from the TMR environment. Further, the program has undergone several other developments including changes to the MPST adjudication process, interstate media coverage and continuous enhancements of system to meet ongoing business needs.

3.2 Project objectives and scope

In light of the changes noted above, TMR and QRO have decided to undertake another PIA, as a matter of privacy best practice.

The below describes the areas in scope for the PIA:

1. Review changes to the MPST adjudication process since the original PIA
2. Change with MPST Unit moving to QRO
3. Changes with scheduling of cameras
4. Functional and technical changes to the existing IAP that have occurred
5. New IAP for QRO
6. Media attention that has arisen and may arise
7. Assess the design of personal information handling practices
8. Confirm privacy risks reported in previous PIA have been addressed, and
9. Assess design of the privacy complaints management process within the MPST Team.

Privacy considerations in respect of other Queensland Road Safety cameras was an area specifically identified to be out of scope for this PIA.

3.3 Project status

The MPST program has been operational since November 2021 and processes have been transitioned to Business as Usual (BAU). The MoG changes have been completed. These include the movement of the MPST Unit into QRO and movement of the MPST Unit to a new building location. The MPST Unit continues to work using systems and applications hosted and maintained by TMR.

Development of the IAP is ongoing. This PIA was largely conducted during the design phase of the new IAP which is part of a 10-week initial planning stage; this was completed on 22 December 2023. The implementation stage commenced 8 January 2024 and the new IAP go-live is scheduled for the end of August 2024.

3.4 Program stakeholders

The key stakeholders in the MPST program are as follows.

3.4.1 QRO

QRO is responsible for:

- The adjudication and service of infringement notices of offences captured by the MPST program
- Partly processing payments (TMR also processes payments)
- Processing of nominations regarding the infringement notices
- Dispute and complaints management related to issued infringement, and
- Other enquiries or issues related to the issued infringement (e.g., fraud, domestic violence).

3.4.2 TMR

TMR, as the party with the administrative responsibility for the legislation enabling the MPST program, currently manages all the arrangements with the camera and AI provider, including camera deployment, all infrastructure and the IT environment for the images coming in. TMR is also responsible for administering non-infringement sanctions (e.g. demerit points), prosecution of offences, transport-related policy and compliance.

3.4.3 IAP Supplier

TMR has engaged a supplier for the development of the new IAP. The IAP supplier will co-design the platform with TMR and QRO, build out the solution and stay on as a managed service provider post-implementation.

The IAP will utilise a third-party software product as the new platform.

3.4.4 Camera and AI provider

The camera and AI provider is engaged to provide the cameras and AI technologies to capture the initial images of a potential seatbelt or mobile phone offence. The supplier has been the provider of the cameras since the start of the MPST program.

IIS did not meet with the supplier for this PIA as consideration of the camera solution was out of scope (and was dealt with in the original PIA).

3.4.5 Community stakeholders

As IIS noted in the original PIA, members of the community are an important stakeholder group as they are directly impacted by the MPST program. They might receive an infringement notice for an alleged distracted driver or seatbelt offence. They are also expected to benefit indirectly via the reduction in road fatalities and injuries.

Social licence – that is, the trust the community gives the government to make laws, conduct programs, provide services and make decisions on its behalf and in its interest – is also relevant here. The obligation rests with government to ensure this licence is not abused.

In light of the recent media attention on the Queensland MPST program and similar initiatives in other states, the sentiments of the community are an especially relevant consideration to the processes of the program.

3.5 Legislative framework

3.5.1 Transport Operations (Road Use Management) Act 1995

The primary legislative authority enabling the administration and enforcement of mobile phone and seatbelt offences is the *Transport Operations (Road Use Management) Act 1995 (Qld)* (TORUM Act) and related Regulations.

3.5.1.1 Camera detected offences

Part 2 Division 2 Photographic detection devices (ss 113-121) of the TORUM Act provides for camera detected offences. Specifically:

- The camera device is an approved photogenic detection device (as prescribed by the *Traffic Regulation 1962* and under s113A of the TORUM Act)
- Failure to use seatbelts, comply with seatbelt requirements and the use of mobile phones are prescribed offences (as per ss 264, 264A and 300 of the *Transport Operations (Road Use Management—Road Rules) Regulation 2009)*, and
- A person is taken to have committed an offence if a prescribed offence happens, and the offence is detected by a photographic detection device (s 114 of the TORUM Act).

The implementation of the MPST program was effected by the *Transport and Other Legislation (Road Safety, Technology and Other Matters) Amendment Act 2020* and the *Transport Legislation (Distracted Driver and Other Matters) Amendment Regulation 2021*. Together this legislation amended the TORUM Act and related Regulations.[1]

The amending legislation:

- Expanded the definition of a mobile phone offence: A driver must not have a mobile phone in their hand or resting on any part of their body, including their lap, while driving – regardless of whether the phone is on or in use. Previously, the rule was that the driver must not use a mobile phone in their hand while driving
- Prescribed mobile phone and seatbelt offences as camera-detected offences
- Made technical amendments to the driver seatbelt offences to enable camera enforcement
- Set out the details of the camera system, including the operational and testing requirements, and the information that must appear on the camera images
- Provided for the deletion of images that do not contain an offence
- Provided for a human (i.e., an authorised officer) to adjudicate on an offence before an infringement is issued, and
- Prescribed corporation penalty amounts for mobile phone and driver seatbelt offences.

Further, the application of the *State Penalties Enforcement Act 1999* (SPE Act) to infringement notices is provided in s 121 of the TORUM Act (see below for further discussion).

3.5.1.2 Confidentiality

Section 143 of the TORUM Act provides confidentiality provisions which are relevant to the MPST program. A person may not disclose, record or use information:

- Through involvement in the administration of the TORUM Act, or
- Because of an opportunity provided by the involvement.

However, an exception exists, and a person may disclose, record or use the information:

- In the discharge of a function under the TORUM Act, or
- If it is authorised—
  - Under another Act or a regulation; or
  - By the person to whom the information relates, or
- In a proceeding before a court or tribunal in which the information is relevant.

[1] Including Transport Operations (Road Use Management – Driver Licensing) Regulation 2010; Transport Operations (Road Use Management – Road Rules) Regulation 2009; and Traffic Regulation 1962.

The *Transport Planning and Coordination Regulation 2017* expands on this exception. Under Part 2A, the disclosure of transport database information is an authorised exception for the purposes of s 143 of the TORUM Act. Sections 10A and 10B of the Regulation set out the conditions for an authorised person to access and use transport information, in order to perform a function under the SPE Act.

Put simply, the above provisions provide the legal authority for MPST team members to access the camera image and prospective offender's details from TMR's Transport Registration and Integrated Licensing Systems (TRAILS) database in order to perform their functions of adjudication and administration for mobile and seatbelt offences. Otherwise, there is a strict duty of confidentiality (unless another exception applies).

3.5.2 State Penalties Enforcement Act 1999

The SPE Act establishes the State Penalties Enforcement Registry (SPER) within QRO. The SPER is responsible for the collection and enforcement of:

- Infringement notice fines
- Court-ordered monetary penalties
- Offender debt recovery orders, and
- Offender levies.

Part 3 of the SPE Act sets out a framework for preparing and issuing infringement notices. Notably:

- Section 13 of the SPE Act provides that: if an authorised person reasonably believes a person has committed an infringement notice offence, the authorised person may serve an infringement notice on the person for the offence, and
- Section 14 of the SPE Act details the service of infringements for offences involving vehicles.

As noted above, the SPE Act applies for infringement notices pertaining to mobile and seatbelt offences under the TORUM Act.

3.5.3 Information Privacy Act 2009

The operations of the MPST program are also subject to the Information Privacy Principles (IPPs) laid out in the *Information Privacy Act 2009* (IP Act).

The IP Act applies to personal information, which is 'information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion' (s 12).

IIS considers that much of the data handled for the MPST program will be personal information in the hands of QRO and TMR.

The IP Act is intended to operate subject to other relevant Queensland laws which may also apply to the collection, use, and disclosure of personal information (s 7(2) of the IP Act). This means that managing the camera footage with personal information involves adhering to both the IP Act and any other applicable legislation. In situations where specific guidance is lacking in these laws, the IPPs will apply to both TMR and QRO/QT, as modified by other legislation, such as the confidentiality provisions of s 143 of the TORUM Act.

Notably, *Information Privacy and Other Legislation Amendment Act 2023* (IPOLA Act) was passed recently and will replace the IPPs and National Privacy Principles (NPPs) in the IP Act with a single set of Queensland Privacy Principles (QPPs). The aim is to better align the privacy principles with the Australian Privacy Principles. These changes will enter into force on 1 July 2025. The IPOLA Act will also introduce a mandatory data breach notification (MDBN) scheme. There is a phased commencement of the MDBN scheme which includes an additional 12-month delayed commencement (1 July 2026) for local governments only.

For the purposes of this PIA – and given the timing of the IPOLA Act is not until 2025 – IIS has applied the existing IPPs. Analysis against individual IPPs can be found in Appendix B.

3.6 System and data components

3.6.1 Transport Registration and Integrated Licensing System (TRAILS) / Transport Integrated Customer Access (TICA)

TRAILS is a database of Queensland vehicle and vessel registration records, driver and marine licence records, industry authority and operator accreditation records, traffic records, customer records and infringement notice records, including personal information associated with these records. There are several ways for staff to access TRAILS.

TRAILS is owned and maintained by TMR. Access to TRAILS by SPER and QRO are provisioned through separate MOUs with the requirements aligning to the SPE Act (the relevant legal authority).

There are integrations in the current IAP which enable TRAILS information to be auto-populated for each incident based on the number plate information of a relevant vehicle. The MPST Unit will still manually access TRAILS/TICA for various reasons, including to verify the information, find interstate drivers or to get further context.

3.6.2 MPST Incident Adjudication Portal (IAP)

The MPST IAP is the central platform for MPST Unit team members to adjudicate individual incidents and administer and manage infringement notices. The current state IAP is a custom-built solution hosted by TMR.

The solution enables automated and UX-based adjudication/verification of incidents by MPST Unit staff, generates the infringement records in TRAILS, and produces corresponding infringement notice and other correspondence to the customer.

The IAP also includes integrations with:

- Camera systems
- TMR Online Services, and
- Print batch processes.

3.6.3 Customer-facing Online Services

There are a number of customer-facing online services which are integrated with the current IAP. These include the option for:

- TMR customers to view the MPST infringement records via the TMR Online Services portal.
- TMR customers to lodge enquiries and nominate another customer or self-nominate, for the infringement using TMR Online Services.

3.6.4 Camera and print batching

Images from the camera and AI provider are stored in a database. Integrations with the IAP run a daily automated batch to securely transfer the images to TMR's database where it can then be accessed by MPST staff via the IAP.

The IAP also integrates with a print batch process. The solution generates dynamically QR coded statutory declaration enclosures, merges them with infringement notice PDFs, and sends them to the mailing house for printing and posting to customer.

3.7 Nature of information and information flows

3.7.1 Nature of information

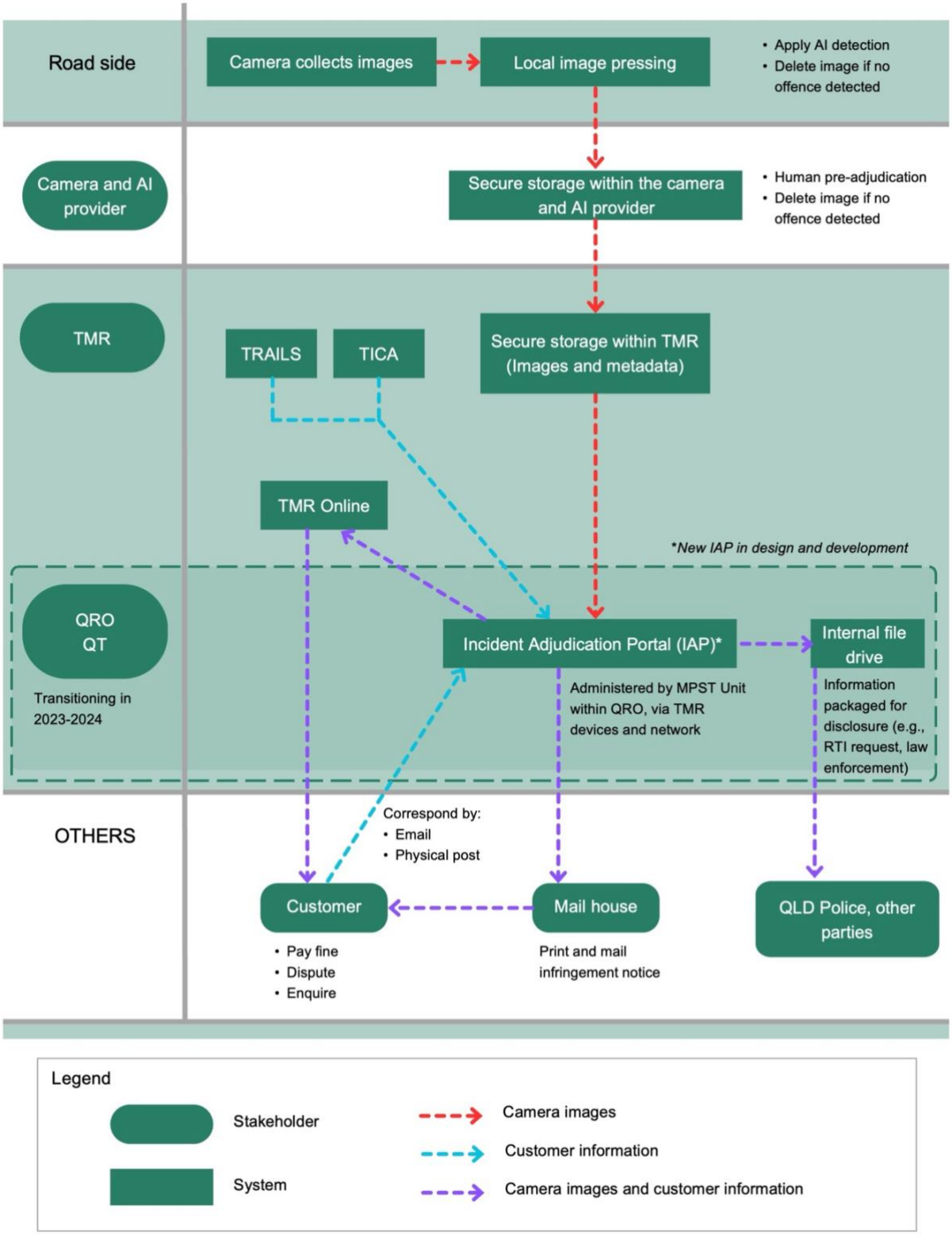
The information the MPST program handles is generally from three sources:

1. **Data captured by the mobile camera** – this involves a set of images of the incident as well as incident metadata. The images capture details of the vehicle (including number plate) and the individuals within the vehicle.
2. **Data accessed on TRAILS/TICA** – this involves vehicle registration details, registered operator details and relevant seatbelt exemptions.
3. **Correspondence from the Customer** – this may involve a wide range of information. Customers may provide the details of another person for nomination, provide details about domestic violence or enquire about the infringement among other things.

In all three cases, IIS considers that the data handled by the MPST Unit is likely to satisfy the meaning of personal information.

3.7.2 Information flow

The following diagram details the high-level personal information flows in the MPST program.



Environment	Description
Roadside	Images (and related data) are captured as motorists drive past a mobile phone and seatbelt camera. AI developed by the camera and AI provider camera flags images for potential incidents. These images are sent to the camera and AI provider while the remainder are deleted.
Camera and AI provider	A human operator provides quality assurance over the AI decision and then releases the images in the camera and AI provider's database. Images with no offence detected are deleted.
TMR	Images in the camera and AI provider's database are securely ingested to TMR's environment. The images are stored within TMR's database while metadata is stored within a separate database.
TMR (IAP)	MPST Unit staff access the incident information stored in TMR's environment via the IAP and adjudicate the incident. Once an incident is accepted and quality assured, an Infringement Notice is created. Staff may also reissue infringements and respond to customer enquiries through the IAP.
TMR (TRAILS/TICA)	The IAP auto-populates certain information from TRAILS. MPST staff may also manually access TICA for driver and vehicle information.
TMR (internal file drive)	Certain incident information may be stored in the MPST Unit's internal file drive. This includes correspondence (e.g., statutory declarations) or information for further disclosure (e.g., RTI request or law enforcement purposes). The management team will also store sensitive incidents in an access-restricted folder in the internal file drive.
Mailing house	Once accepted, the infringement notices are sent to a contracted mailing house as part of its managed service. The infringement notice is printed and issued by mail.
Customer	The customer receives notice. The customer may pay the fine, nominate or enquire. Should the customer reply with correspondence, it will be captured and stored on the IAP and may be stored on the internal file drive. Customers may respond by physical or electronic mail or through the customer facing online-services which are linked with the IAP.
Other (if applicable)	Disclosure of information is provided to other parties from the internal file drive (e.g., RTI request, Queensland Police).

4. Approach to risk analysis

In undertaking this PIA IIS considered:

- The previous PIA report conducted by IIS
- The IPPs and other legislative requirements
- Guidance materials published by the OIC
- Privacy best practice stemming from IIS's knowledge and experience.

4.1 Inherent privacy risks

IIS's risk analysis approach begins with identifying the inherent privacy risks. Inherent privacy risks arise from:

- The nature of the personal information to be collected and managed – for example, its quantity, sensitivity, and the potential for, and consequences of, misuse
- The range of people from whom the information may be collected
- The context in which personal information is handled at TMR and QRO, as well as by its vendors – for example, senior management commitment to privacy, staff privacy skills and experience, the technical systems involved and the nature of the MPST program
- The extent to which information is accessed or handled by third parties, and
- The likely community and/or media interest in the privacy aspects of the MPST program.

Considering these points, IIS considers that the MPST program has a **high** degree of inherent privacy risk because:

- The MPST program is a form of surveillance, which by its nature is privacy intrusive
    - There is potential for harm or embarrassment to individuals, particularly if they are wrongly identified as infringing the Queensland road rules or are caught in illicit or embarrassing behaviour
- The cameras collect images and information on a broad range of the Queensland population as well as interstate and overseas drivers; and, depending on where they are deployed, may be seen to capture images and information that targets a segment of the population
- The MPST program is in a state of transition, with its team having transitioned organisationally and physically, along with a new IAP in development – key processes and IT systems underpinning information handling are still being bedded down
- Once the new IAP is in place, MPST program information may be handled by the IAP supplier as the managed service provider, and
- There has been, and will likely continue to be, community and media interest in the MPST program due to the perceived intrusiveness of the surveillance.

4.2 Positive privacy aspects

IIS has also identified positive privacy aspects of the MPST program, including that:

- The program continues to maintain the protections outlined in the 2022 PIA:
  - The collection and use of images is authorised by law
  - Images are deleted quickly from cameras and from the camera and AI provider's systems, once an offence is ruled out
  - Decisions about offences are not automated, but validated by multiple points of human review
  - People are given copies of the 'offending' images and have the right to seek a review of the decision or to challenge it in court
- The camera and AI provider continues to improve the accuracy and consistency of AI image decision-making
- Access to the IAP is subject to a range of organisational and technical controls
- The MPST Unit has been operational for approximately two years, and has developed ways of working to appropriately handle the information that it collects
- The MPST Unit has its own segregated work space which reduces inadvertent exposure to non-MPST staff
- There is widespread recognition among QRO program management and leadership of the importance of privacy.

4.3 Residual privacy risk level

Overall, the MPST program has been operating smoothly in BAU, albeit with some negative media attention (discussed further below). The recent and incoming changes – including the MoG changes, physical move to a new office, and design and development of a new IAP – present opportunities for the MPST Unit to uplift its privacy practices, procedures and systems.

With several important issues to manage as the new IAP is developed and rolled out, IIS considers the residual privacy risk is **medium**. Privacy risks are likely to be within manageable levels. IIS has made recommendations in the following areas that, If implemented, would reduce the residual privacy risk:

- Further access controls and audit practices
- Strengthened retention and deletion practices for images and personal information
- Better documentation of policies, standards and procedures, with accompanying training
- Further privacy risk due diligence for the new IAP.

5. Findings and recommendations

This section sets out IIS's findings on the following areas agreed to be assessed as part of the PIA scope:

- **Review of 2022 PIA report**
  - Confirm privacy risks (and associated recommendations) have been addressed
- **Business processes, practices, policies and organisational aspects**
  - Changes to the MPST adjudication process and the MPST Unit's move to QRO
  - Design of personal information handling practices and privacy complaints management process
- **System (technical) components and data**
  - Functional and technical changes to the existing IAP that have occurred
  - Changes to camera scheduling
  - New IAP for QRO
- **Other issues**
  - Media attention and public expectations.

For each area, IIS discusses the key issues and privacy risks. Where we have identified a risk to be mitigated (including, but not limited to, non-compliance with the IPPs), we provide a **recommendation**. Where we have identified an area for improvement, we provide a **suggestion** for best practice.

A high-level assessment against the IPPs is at Appendix B.

5.1 Review of 2022 PIA Report

As this PIA is a follow-up to the 2022 PIA, TMR and IIS considered that it would be worthwhile to revisit the privacy risks and recommendations arising from the previous report and confirm that they have been adequately addressed.

The 2022 PIA recommendations focused on matters of privacy governance – both generally at TMR and specifically for the MPST program – and alignment of personal information handling practices with the IPPs. For ease of reference, we have listed the recommendations along with their status in the following table:

2022 PIA recommendation	Status
Rec 1 – In consultation with the Privacy Team, formalise TMR's policy position on use of AI in decision-making. Include in particular: 1) TMR's position on ensuring 'human in the loop' decision-making; and 2) associated requirements to consider the probability and severity of privacy (and other relevant) harms.	**No longer applicable.** Rather than developing TMR-specific AI policies, TMR has contributed to whole-of-government initiatives, including the Queensland Government Customer and Digital Group (QGCDG) and AI resources under development.
Rec 2 – In consultation with the Privacy Team, formalise MPST-specific governance. Include specific policies, procedures and accountabilities for: 1) expanding offences to be detected using the MPST cameras; 2) combining the camera technology with other technology (e.g., speed detection, facial recognition); and 3) details of the existing TMR processes for managing requests from law enforcement bodies and others to access, use or disclose images for non-MPST purposes.	**Completed.** There will be no expansion of offences or technological uses without the approval of Queensland government and relevant governance bodies. A document policy is in place for TMR to manage law enforcement requests to images obtained from the MPST program.
Rec 3 – Monitor decisions about MPST camera placements for patterns that could be construed as responsive to community characteristics (e.g., demographics, socio-economic). Take proactive steps to address related perceptions of program bias, such as through community outreach and other communications initiatives.	**Completed.** The selection of camera placements is documented and based on crash data, regardless of community characteristics. TMR will investigate opportunities as part of its existing consultative and public awareness activities to consider the need to address possible perceptions of program bias.

2022 PIA recommendation	Status
Rec 4 – Report MPST outcomes to the community at regular intervals. In addition, publish findings of any program evaluations undertaken.	**Not fully addressed.** There has been no specific reporting of MPST outcomes. MPST has been considered in broader road safety research reports.[2] MPST is one of many types of camera-based traffic enforcement, as part of TMR's Camera Detected Offence Program (CDOP). However, the last evaluation of CDOP was for 2018-2019, before MPST cameras were introduced. IIS understands that the Qld Road Safety (QRS) Board, the successor to CDOP, will be completing a review of the objectives outlined in the Queensland Road Safety Strategy in the 2024 calendar year. TMR will liaise with the QRS program management office to confirm dates and the extent to which the review will address MPST.
Rec 5 – Conduct a further PIA on MPST within one year of commencing the enforcement phase.	**Completed (this PIA).**
Rec 6 – Conduct a PIA where it is proposed to expand the use or functionality of MPST cameras, and/ or where there is a significant departure from the present MPST program specifications.	**Completed (for ongoing consideration).** The CDOP will conduct a PIA in consultation with the privacy team if there is any intention to expand the use of MPST cameras.
Rec 7 – Review TMR's policy position in the context of Recommendations 3 and 4 on: 1) deciding MPST camera locations and 2) monitoring decisions for perceived bias.	**Completed.** TMR is in the process of developing a new camera scheduling solution. See further discussion in Section 5.3 below.

[2] See TMR, 'Road safety research reports' (11 December 2023) <https://www.tmr.qld.gov.au/safety/road-safety/road-safety-strategy-and-action-plans/road-safety-research-reports>.

2022 PIA recommendation	Status
Rec 8 – Explore with the Privacy Team opportunities for the MPST Adjudication Team to receive tailored training about privacy considerations specific to their role.	**Completed.** MPST privacy training was developed by the TMR Privacy Team in 2022. However, given changes to the operations and structure of the MPST Unit, it would be worthwhile to develop additional training. See Section 5.2.3.2 below for further discussion.
Rec 9 – Continue to promote the MPST program through various communication channels to ensure community awareness that their personal information may be collected remains high.	**In progress.** TMR will consider mobile phone and seatbelt offences when planning future public awareness campaigns to ensure awareness remains high.
Rec 10 – Update TMR Privacy Policy to include reference to camera-enabled offence detection and the collection of relevant images. Consider direct reference to the MPST program or providing a link to surveillance-related resources.	**Completed.** This information has been included in the August 2022 update of TMR's Information Privacy Plan, which is referenced in TMR's Privacy Policy. TMR continues to maintain a webpage that contains general information about mobile phone and seatbelt cameras,[3] including reference to privacy. As a matter of best practice, it may be useful to provide a link in the 'Your privacy' section back to TMR's Privacy Policy.
Rec 11 – Continue proactive disclosure of information about TMR operations through publication of MPST-specific information on the TMR website, either on a dedicated webpage or within existing surveillance-related resources. Additionally, ensure the material published about the MPST program is up to date, specific about the personal information collected and handled for MPST purposes and that key terminology is defined to avoid confusion in the community.	**Completed (for ongoing consideration).** TMR will review the web page content at least every six months and will update where necessary to ensure information is up to date.

[3] TMR, 'Mobile phone and seatbelt cameras' (14 December 2023) <https://www.qld.gov.au/transport/safety/fines/cameras>.

2022 PIA recommendation	Status
Rec 12 – Continue training the AI in the MPST cameras to correctly detect mobile phone use and seat belt offences, whereby irrelevant images (those indicating no offence) are not retained for the adjudication process.	**Completed.** The managed services contract with the camera and AI provider (the vendor of the AI product) includes a range of key performance indicators (KPIs) that need to be met or exceeded. This includes continuous improvement to AI accuracy throughout the life of the contract. This is monitored on a quarterly basis.
Rec 13 – Continue to implement recommendations arising from the TMR Information Security Risk Assessments of the MPST program.	**Completed (for ongoing consideration).** This is considered as part of each change release cycle.
Rec 14 – Routinise the receipt of vendor audit logs associated with the pre-adjudication process.	**Completed.** TMR Principal Advisor conducts audits of vendor's pre-adjudication process on a regular basis.
Rec 15 – Urgently open discussions with the MPST program Board to: 1) communicate a requirement for a secure-access facility accessible only to the MPST Adjudication Team; and 2) seek resolution to accommodation issues prior to 30 November 2021.	**Completed.**
Rec 16 – Urgently address physical security considerations and operational challenges relating to accommodation by: 1) relocating to the same floor within TMR until a secure-access facility is made available; 2) moving adjudicator desks out of high traffic/thoroughfare areas; 3) positioning adjudicator desks so that monitors are not able to be viewed 'over the shoulder'.	**Completed.**

2022 PIA recommendation	Status
Rec 17 – Seek urgent advice of the Privacy and Records Management teams as regards secure destruction of (or management as 'records' of TMR, if required) any MPST images and associated commentary shared amongst adjudicators within the Microsoft Teams environment.	**Completed.** TMR confirms the images and associated commentary have been deleted.
Rec 18 – Conduct longitudinal analysis of accuracy of QA adjudicator decisions (with learnings to be incorporated into MPST adjudication processes) and report on findings.	**Not fully addressed.** Quality assurance arrangements are in place for adjudication decisions. However, there has not been longitudinal analysis of the accuracy of QA adjudicator decisions.
Rec 19 – Where a passenger seatbelt offence **is not** detected by an MPST camera, take steps to limit visibility of (or entirely obscure) passenger images through the further adjudication processes relating to the driver and any subsequent issue of infringement notice.	**No longer applicable.** TMR has investigated this issue and considered that the technical effort involved in taking further steps is disproportionate to the potential benefit. IIS notes that TMR has introduced a pixelate feature. We discuss its potential use in Section 5.4.1 below.
Rec 20 – Where a passenger seatbelt offence **is** detected, investigate whether passenger face (where visible in whole or in part) can be obscured when generating the infringement notice.	**No longer applicable.** TMR requires the passenger face to be visible so the registered operator can identify who the person is to check if a seatbelt exemption applies.
Rec 21 – Where the Regulations do not specify additional permitted **uses** of MPST images and other personal information, follow the overarching privacy governance requirements for MPST. Refer also: Recommendation 2.	**Completed (for ongoing consideration).** TMR will continue to follow overarching privacy governance and legislative review requirements.
Rec 22 – Where the Regulations do not specify additional permitted **disclosures** of MPST images and other personal information, follow the overarching privacy governance requirements for MPST. Refer also: Recommendation 2.	**Completed (for ongoing consideration).** As above.

5.2 Business processes, practices, polices, and organisational aspects

This subsection examines business and organisational practices pertaining to the MPST program and its management of personal information, with a focus on the MPST Unit. The MPST Unit accesses TMR information to perform its duties of adjudicating camera-related offences and issuing and managing infringement notices.

From a privacy compliance perspective, the primary considerations for the MPST Unit are IPP 4 (storage and security of personal information) and IPPs 9-11 (use and disclosure of personal information).

IIS heard throughout interviews that a misuse of the images by an authorised user would also have the potential to significantly impact public trust. Therefore, the risk to be mitigated when considering the MPST Unit's business and organisational practices can be described as: **Unauthorised access to or misuse of TMR information by staff, contractors or third parties resulting in non-compliance with the law, harm to the customer, reputational damage to government and eroded public trust**.

5.2.1 Changes to the MPST adjudication process

5.2.1.1 User roles and responsibilities

User roles and access to information

At the time of conducting the previous PIA (late 2021 to early 2022), the MPST Unit was still in early stages of operations. Since then, the MPST Unit's operations have matured, with defined team roles and responsibilities. The MPST Unit comprises four teams, representing distinct stages of the workflow lifecycle:

- **Adjudications** – Manual review of camera images, prepare infringement notices
- **Nominations** – Receive statutory declarations and other nominations and reissue infringement notices
- **Client Support** – Respond to customer enquiries about their infringement/s
- **Operations** – Manage customer enquiries and issues that require escalation.

All MPST Unit staff have read and write access to the IAP to perform their duties. A small number of users from the TMR Prosecutions Unit have read-only access to the IAP.

IIS understands there are no technical limitations on team members' access to the IAP from a workflow lifecycle and system perspective. That is, team members who work on manual review of camera images (i.e., typically in the Adjudication Team) can access customer correspondence (i.e., in the Client Support team), and vice versa. The practical limitation is business procedure.

Other recent changes to the IAP in terms of user roles relate to admin-level functionalities that the MPST Unit restricts to team leaders and managers. These are implemented at a technical level, and include:

- Dashboard reporting
- Modify the SPER fees and statutory declaration address on infringement notices
- Turn pixelation capability on and off
- Access audit logs
- Add or remove flags, and
- Add or amend templates and inserts.

In discussions with the MPST Unit, IIS was informed that team members are occasionally granted temporary admin-level access to assist with reporting or to act in a higher duty temporarily. Such access is revoked once it is no longer required.

IIS considers the admin-level functionalities to be appropriate and has not identified any issues with how they are implemented. We do, however, have some concern with the current business practice of team members having full access to the IAP, even for functions that are outside of their roles. While it may be useful as a matter of efficiency for team members to have full access, this appears to be more a reflection of the limitation of the existing IAP rather than an intentional design element.

Furthermore, allowing full access goes against the principle of least privilege and heightens the risk of unauthorised access and misuse. IIS considers that more granular access settings should be explored as part of the new IAP. As part of this, it would be worthwhile for team leaders to discuss which functionalities throughout the workflow lifecycle should be available generally to which teams, and which ones can be granted by way of exception.

Recommendation 1 – Explore more granular access settings for MPST Unit staff, as part of new IAP
Define key functions and activities in the MPST workflow lifecycle, including which teams are responsible for what. Implement more granular access settings (via both technical and business means) so that MPST Unit staff only access the IAP functions that they need to perform their roles, with exceptions as necessary. **Who:** QRO and IAP supplier **When:** Before go-live of new IAP

Auditing function and practice

Related to access settings based on user roles and responsibilities is how they are enforced and checked over time. IIS understands that one of the recent technical changes to the existing IAP was the introduction of improved audit logging, with the capability to review user activities. This was introduced following an internal case of unauthorised access and disclosure of camera images, which highlighted shortcomings with audit logs in the IAP at the time.

IIS notes that having the technical capability for auditing is not sufficient on its own. It needs to be accompanied by supporting policy and practice. We understand that, previously, the MPST Unit would only perform audits reactively, when it was notified of an issue. At the moment, an MPST manager or team leader conducts ad hoc checks, for example when they become aware that a team member's behaviour warrants checking. There is no formalised audit policy or practice.

In discussions with the MPST Unit, IIS has become aware of certain challenges with respect to auditing. Firstly, there is limited capacity for managers and team leaders to conduct manual audits. In order to have a semi-regular auditing function, it may be necessary to define an explicit role or responsibility to perform it, that is appropriately resourced. Secondly, there is the practical difficulty of ascertaining what is wrongdoing, given that team members are accessing hundreds of incidents (with associated images and customer information) per week.

Nevertheless, given the risk context and the potential sensitivity of the camera images, IIS considers that a reasonable step for the MPST Unit to take under IPP 4 is to develop and implement an audit policy and procedure.

A starting point would be for team leaders to discuss and agree on particular behaviours or patterns of conduct that an audit policy should look out for. For example, this could relate to the quantity or timing of IAP usage, or the extent to which incidents with comments or particular tags are being accessed.

The frequency of auditing would depend on the practicality and effort involved. IIS considers that it would be reasonable for a sample of every team leader and member's activity logs to be reviewed at least once per year, with additional ad hoc checks as necessary. This would be a good opportunity to also conduct access reviews to ensure staff permissions are current and relevant.

Recommendation 2 – Review and update formal audit policy and procedure for the IAP

Review and update audit policy and procedure for users of the IAP, taking into account:

- As a practical matter, the kinds of behaviours or patterns of conduct to focus on
- Roles and responsibilities in the audit process
- The cadence of regular audits (at a minimum, annually for each user of the IAP).

Ensure there is appropriate resourcing for the audit policy and procedure to be operationalised.

Who: QRO

When: Within 6 months

5.2.1.2 MPST Unit moving to new physical location

Prior to the MoG change, the MPST Unit, as part of TMR, moved to a location in the Brisbane central business district on 4 July 2022. The MPST Unit occupied one side of the floor. Efforts were taken to minimise inadvertent screen exposure to non-MPST staff on the same floor. For example, communications were sent between departments suggesting that non-MPST staff should only walk to the male bathroom through the shared space rather than walking the length of MPST side of the floor. Privacy screens were also trialled though not fully implemented.

On 20 November 2023, the MPST Unit moved again, this time as part of QRO, to a new location. Similarly, the team occupies one end of the floor to minimise inadvertent exposure by non MPST staff. The MPST Unit informed IIS that it will have its own storage and mail rooms in this new location.

Overall, IIS considers that the new location and floor plan is an improvement on previous locations. We encourage the MPST Unit to practice good physical security controls and be proactive in limiting inadvertent exposure to non-MPST staff.

5.2.2 MPST Unit's move to QRO

5.2.2.1 Implications of move to QRO

Organisationally, the MPST Unit transitioned from TMR to QRO on 30 November 2022 as part of MoG changes. Aside from the move to a new physical location outlined above, there has been little impact to its operations. This is because the MPST Unit continues to use TMR devices, credentials and network to conduct its work. The existing IAP, as well as TRAILS and TICA, are maintained and hosted by TMR, and access is provisioned by TMR's Service Centre Online (SCO). The MPST Unit must undertake TMR training with respect to TICA, Information Privacy and Ethical Decision Making as part of the onboarding process.

IIS understands that the primary change to date is that the MPST Unit, as a team within QRO, is subject to QT's information privacy framework. This includes annual mandatory privacy training for all staff, as well as adherence to an internal privacy breach and complaints procedure. We have not identified any other changes to the team arising from QRO practice and culture.

The MoG changes relating to the MPST is also significant from the perspective of QRO and QT. One MPST Unit stakeholder observed that the potential invasiveness of the camera angles and quality of camera images involved is something that QRO and QT have not had to deal with previously. IIS discusses co-governance between TMR and QRO/QT further below.

There are plans underway to further transition the MPST Unit in 2024, in terms of using QT's devices, software licences and a new IAP hosted within the QRO/QT environment. IIS considers that these changes do not meaningfully change how the MPST Unit will handle TMR information, and therefore do not raise any additional privacy issues. Users will still require access to camera images, TRAILS and TICA, and will continue to be subject to both TMR and QT policy overlays.

5.2.2.2 Governance

Given the centrality of TMR information to the MPST Unit's operations, it is important that there are clearly defined roles and responsibilities for both TMR and QRO in the co-governance of this information. This has been formalised in two key MOUs:

- MOU between TMR and SPER for Information Exchange (July 2020) and accompanying Information Exchange Schedule (SPER/0001) (July 2022)
- MOU between TMR and QRO for Fine Administration and Management Services (May 2023) and accompanying schedules.

IIS summarises the relevant provisions as follows:

Governance document	Relevant provisions
TMR-SPER MOU	• General commitment to purpose and access limitation, reporting and managing incidents (including privacy and security breaches), maintaining information quality, and securing information, as outlined in the information exchange schedule.

Governance document	Relevant provisions
Information Exchange Schedule	• Sets out the approved purposes for SPER to obtain, access and use TMR information (including serving infringement notices, and administering and enforcing infringement notices and enforcement orders) • Specifies TMR as the owner, data custodian and incident manager[4] of the information that is shared • Defines systems access controls for authorised persons • Sets out high-level incident management steps – SPER to report any incidents (breaches, access issues, security issues) to TMR as soon as practicable; all parties will work together to investigate any alleged or suspected information security breaches • Sets out reporting and audit requirements for SPER – on request by TMR, and at least annual attestation of compliance with information security and audit requirements • Sets out the applicable Queensland policies and frameworks for information security.

[4] Defined in the TMR-SPER MOU as 'The person responsible for the resolution of any information security incidents.'

Governance document	Relevant provisions

TMR-QRO MOU and Schedules (especially Schedule 2 – Support Services)	• Part B.2 – Business Support Services
	  ○ Allocation of responsibilities between TMR and QT for MPST, including that TMR will act as sole liaison point with the camera technology vendor for all contract-related matters
	• Part C – Information Technology Services
	  ○ All access to and use of data from TRAILS and TICA must be in accordance with the TMR-SPER MOU and its Information Exchange Schedule
	• Part D – Information Sharing and Transfer of Information
	  ○ The TMR-SPER MOU and its Information Exchange Schedule will continue to apply to the exchange of other information held and shared by TMR
	  ○ Further defined responsibilities for TMR and QT in relation to information access and sharing
	  – Notably, QT must restrict access to information only to staff who requires it to perform Fine Administration and Management Functions, and such access is audited regularly
	  ○ Where information includes personal information, the parties will work cooperatively to:
	  – Identify and enable the relevant entity to respond to privacy complaints, access or amendment applications
	  – Investigate, manage, contain and notify stakeholders following a privacy breach.

IIS finds that the MOUs sufficiently cover matters that are relevant for cross-agency information exchange from a privacy and security perspective. In particular, there are clear provisions relating to how the parties should respond in the event of a security incident or privacy breach.

A key consideration is how well the provisions are operationalised, especially in the context of MPST. In conversations with MPST and QRO stakeholders for the PIA, IIS encountered uncertainty and different understandings around whether, when and how to report to TMR in the event of a security incident or privacy breach. This could be due to a lack of familiarity with the MOU provisions, as well as a lack of formalised operational procedures.

IIS understands that QT has a general privacy breach procedure and is in the process of finalising a 'playbook' for how to deal with more serious privacy and security breaches. Given the risk context, we consider that it is worthwhile for the MPST Unit to formalise its own procedure for responding to privacy and security incidents and breaches, including reporting to the TMR and QT privacy officers (see Section 5.2.3.2 below for further discussion on policies, standards and procedures).

As part of this process, the MPST Unit, along with the TMR and QT privacy officers, should collaborate on what the procedure should look like, and how it aligns with the respective agencies' existing overarching policies. The goals should be to:

- Have a common, documented understanding of how to respond to incidents and breaches arising from the MPST Unit
- Build awareness among key stakeholders for what to do, and
- Foster a positive working relationship between TMR and QRO/QT on privacy matters.

Suggestion 1 – Review and update existing procedures and implement updated policies, while fostering working relationship for responding to MPST privacy and security incidents and breaches

Develop a documented procedure for responding to privacy and security incidents and breaches, in the context of MPST. Gain input from TMR and QT privacy officers. Ensure all stakeholders are aware of the procedure.

Maintain regular lines of communication between TMR and QRO/QT for privacy matters to be raised and addressed.

Who: TMR, QRO and QT

When: Within 6 months and ongoing

5.2.3 Design of personal information handling practices

5.2.3.1 Personal information handling processes

IIS was asked to consider the personal information handling in place for the adjudication process, including follow-up processes for unpaid infringement notices. In this sub-section, IIS focuses on several areas where we have identified potential issues with personal information handling.

Retention of images where there is no offence

Camera images received by the MPST Unit for adjudication have already gone through two levels of pre-adjudication. Firstly, there is local AI processing on the camera and, secondly, there is human review at the camera and AI provider. Where no offence is detected, the image is deleted from the camera or the camera and AI provider's system after a short period as a privacy-preserving feature.

The Adjudication Team within the MPST Unit will undertake two rounds of human review to confirm that a mobile phone or seatbelt offence has been committed. IIS understands that regardless of whether an offence has been committed, the current practice is to store all camera images in the IAP.

The MPST Unit informed IIS that there are several reasons for retaining camera images:

- Where an offence has occurred:
  - To maintain records as part of the fine administration process – this would include the infringement notice and associated camera images and incident information
  - To maintain records where the incident has been rejected for some other reason.
- Where an offence has not occurred:
  - To assist with investigations into fraudulent nominations – e.g., comparing driver appearance where there have been multiple detections of the same vehicle
  - To assist in dealing with other matters of concern, such as domestic and family violence (DFV).

While there may be legitimate reasons for retaining images, including where an offence has not occurred, we caution the MPST Unit against retaining all images indefinitely by default. Such a stance would be counter to the data minimisation approach that is already applied at other points in the MPST data lifecycle. It would lead to a 'honeypot' of information that comes with increased risk of unauthorised access and misuse, as well as function creep, where the images or technology are used in new ways that might be unexpected or unwelcome to the community.

Investigating fraudulent nominations through reviewing camera images has a tangible connection to the MPST Unit (since dealing with nominations is part of its remit). However, this capability means it is possible to conduct all kinds of other potential investigations, especially given the high quality and quantity of the images, coupled with the IAP's search functionality. This increases the risk of function creep, especially in relation to investigatory purposes.

Given the risk context, IIS considers that the default position should be that camera images and associated metadata are deleted if: (i) there are no offences detected in the image, and (ii) there are no other legitimate business reasons to retain them, as connected with the MPST program's objectives and as authorised under the TORUM Act.

The MPST Unit should determine and document the specific business reasons for retaining camera images, including time limits for how long they need to be retained. Where there are practical or policy reasons that would prevent permanent deletion, the MPST Unit should consider other ways of making camera images unavailable, such as archiving in an area that is removed from ordinary access. This could be explored in the design of the new IAP and in subsequent releases.

Recommendation 3 – Review and update formal policy for retention and deletion of camera images

Review and update policy for retention and deletion of camera images, taking into account:

- Specific business reasons for retaining camera images
- Time limits for how long they need to be retained
- The manner of deleting or otherwise disposing of the camera images.

Delete or otherwise dispose of camera images in accordance with the policy.

Who: QRO

When: Within 6 months

IIS understands that in implementing data disposal practices, TMR and QRO will need to assess the new IAP to ensure that the decoupled solution is technically capable of complying with applicable disposal policies and schedules. This body of work will follow the completion of **Recommendation 3**.

Retention of personal information in email inboxes

Following adjudication and issuing of the infringement notice, the MPST Unit can receive further information from customers as part of the workflow lifecycle. This includes:

- Posting back a completed statutory declaration nomination form or completing it online
- Sending an enquiry (or other comments and feedback) via email or post.

IIS understands that physical forms are scanned and automatically saved into an MPST email inbox, before being uploaded to the IAP.

The information being collected and retained by MPST email inboxes includes personal information, such as names, contact details and addresses, along with other potentially more sensitive information about customers (e.g., where they have self-reported health conditions or safety/welfare issues as part of challenging an infringement notice).

IIS notes that absent of any additional steps, the MPST Unit will continue to accumulate information in its email inboxes over time. This contributes to unnecessary retention of personal information and heightens the risk of unauthorised access and misuse. We consider that a reasonable step for the MPST Unit to take under IPP 4 is to develop and implement an email retention/archive policy.

Recommendation 4 – Review and update email archive/retention policy

Review and update an email archive/retention policy for MPST email inboxes that sets out:

- A defined period for keeping emails in the main inbox
- A method for archiving or otherwise disposing of emails following this period.

Archive or otherwise dispose of emails in accordance with the policy.

Who: QRO

When: Within 6 months

Processes for handling sensitive images

IIS understands that due to the indiscriminate nature of image capture from roadside cameras, the MPST Unit will receive camera images that depict individuals in a range of circumstances while driving on Queensland roads. These include nudity, sexual activity, drug use, weapons, DFV, other kinds of criminal activity, etc.

With respect to these sensitive images, the MPST Unit is conscious of the need to minimise access to sensitive images from both a staff welfare perspective and to reduce the risk of unauthorised access and misuse. However, a current challenge is that where such situations arise, multiple people may need to be exposed to sensitive images, as a matter of applying the adjudication rules and later as part of quality assurance steps.

During consultations, IIS discussed with MPST Unit stakeholders the prospect of further locking down access to sensitive images. We understand that this could be implemented as a feature in the new IAP. For now, the MPST Unit's current practice is for users to tag such images as a 'matter of concern' (or where relevant, 'DFV'). Furthermore, a user can add a comment to the incident file, to warn others about not clicking into the images.

Stakeholders noted that there are pros and cons with the current method. On the positive side, the tags and relevant comments would help to warn other users about potential sensitive images to avoid them. On the negative side, the tags also make it easier for a bad actor to find such sensitive images. Rather than going on a 'fishing expedition', they could search or filter by 'matter of concern' to find such images, thereby defeating the protection granted by 'security through obscurity'. IIS notes that this can be addressed by an audit regime that examined such behaviours (see discussion at Section 5.2.1.1 above and **Recommendation 2**)

Given the shortcomings with the current approach, IIS considers that a feature for flagging and restricting access to sensitive images (e.g., only to MPST Unit team leaders and other approved users) should be explored for the new IAP.

Recommendation 5 – Explore feature for flagging and restricting access to sensitive images in the new IAP
Explore option for introducing the capability to flag and restrict access to sensitive images, as part of design and development of the new IAP. **Who:** QRO and IAP supplier **When:** As part of subsequent releases following go-live of the new IAP

5.2.3.2 Policies, standards and procedures

MPST Unit documentation

IIS was also asked to assess the policies, standards and procedures as they pertain to the MPST Unit's personal information handling practices. Overall, we find that documented policies, standards and procedures within the MPST Unit are under-developed, especially given the risk context and the kinds and amounts of personal information that it handles.

As part of this engagement, the MPST Unit shared with IIS:

- Conflict of Interest Procedure, which applies to the Fine Administration and Management (FAM) Division that the MPST Unit is a part of
- Matters of Concern Procedure for the MPST Unit (in draft)
- Induction and training material (in presentation slides) for the MPST Unit – IIS further discusses training below.

While the documents addressing conflicts of interest and matters of concern are useful and important, they do not provide adequate coverage of the kinds of information handling activities performed by the MPST Unit across the workflow lifecycle.

Based on interviews with MPST Unit stakeholders, it is apparent that team members and leaders handle personal information not just within the IAP but also in other contexts:

- Access to TRAILS and TICA to obtain customer information
- Handling of various operational matters within their internal collaboration software (which could involve spreadsheets with names and incident numbers)
- Handling of various kinds of information that is saved to, and shared from, the internal file drive (e.g., scans of statutory declaration forms, ministerials, RTI requests, external media requests, matters of concern).

IIS considers that the MPST Unit operates with professionalism and care. However, there appears to be a heavy reliance on MPST team leaders with knowledge and experience of the way things work. This is a risk as they represent single points of failure. Furthermore, a lack of documented procedures could lead to human error in how personal information is handled and heighten the risk of unauthorised access and disclosure.

The MPST Unit should begin the journey of formalising its processes and procedures, noting that progress may be slow due to its other commitments. MPST Unit team leaders should discuss and agree on which processes and procedures to prioritise, taking a risk-based approach. IIS has also made recommendations and suggestions pertaining to reviewing and updating certain policies and procedures throughout this PIA:

- **Recommendation 2** – Formal audit policy and procedure for the IAP
- **Recommendation 3** – Formal policy for retention and deletion of camera images
- **Recommendation 4** – Email archive/retention policy.

Recommendation 6 – Develop formalised processes and procedures that cover the MPST Unit's workflow lifecycle, as prioritised using a risk-based approach

Define key functions and activities in the MPST workflow lifecycle, taking a risk-based approach to prioritise the processes and procedures that should be documented.

Develop formalised processes and procedures that cover the MPST Unit's workflow lifecycle. At a minimum, this should include:

- Protocols for:
  - Using the various systems that hold personal information
  - How to safely access, use, disclose and otherwise handle information across these systems
  - How personal information is to be shared with third parties, including law enforcement
- Responding to privacy and security incidents and breaches (see also **Suggestion 1**)
- Finalising the Matters of Concern Procedure, including clear instructions on how team members should deal with, and report, sensitive images.

Who: QRO

When: Within 6 months, to be revisited when significant changes occur (e.g., transition to new IAP, transition of devices/environments to QT)

MPST Unit training

IIS understands that new starters to the MPST Unit must undertake a series of online training modules. As noted above in Section 5.2.2.1, due to the current organisational arrangements staff must undertake both TMR training and QRO/QT training. These cover similar general topics including privacy, information security and code of conduct. There is also specific training for TICA as a condition of gaining access. We understand that TMR is in the process of rolling out further training for access to TRAILS, which was one of the outcomes of Operation Impala that reported on misuse of confidential information in the Queensland public sector.

There is no online module for MPST-specific training. Rather, new starters are onboarded through a multi-day, face-to-face induction program. IIS has reviewed the training schedule and presentation slides. The induction covers:

- General welcome and corporate induction
- Technology set-up and staff expectations
- Infringement lifecycle
- Introduction, live demonstration and buddying/practice for:
    - Adjudication (overview)
    - Mobile Phone adjudication
    - Seatbelt adjudication
    - TICA
    - Interstate adjudication
    - Quality Assurance
    - Deployment validation
    - Seatbelt exemptions.

The presentation slides are clear, thorough and informative.

IIS observed that neither the induction content nor presentation slides specifically addressed information handling, privacy or security. An MPST Unit manager informed IIS that MPST-specific content is delivered after the new team members have completed the generic privacy, information security, ethical decision-making training modules. Further, it was suggested that these topics would be raised organically as part of discussions and demonstrations. We consider that these topics could be more directly contextualised to the MPST Unit and be covered specifically as part of the training content, given the risk context and the sensitivity of images and information that staff are dealing with.

The specific training content should correspond to, and reference, the kinds of documentation to be developed by the MPST Unit as part of **Recommendation 6** above.

Recommendation 7 – Review and update specific information handling, privacy and security training content as part of MPST induction

Develop and roll out specific training content on information handling, privacy and security as part of MPST induction.

Align the content to the formalised processes and procedures to be developed as part of **Recommendation 6**.

Who: QRO

When: Within 6 months, to be revisited when significant changes occur (e.g., transition to new IAP)

5.2.4 Privacy complaints management process

In discussions with MPST Unit stakeholders, IIS gained an understanding of customer complaints and enquiries that are handled by Client Support staff, which can be escalated to the Operations team. The MPST Unit receives regular, daily correspondence from customers. The kinds of complaints and questions include:

- Challenging the right for the state to take an image of them in a private vehicle
- Asserting the legislation doesn't apply to them, or asking which legislation applies
- Asking how QRO got their address, or raising that their address is incorrect
- Raising privacy concerns about the camera image.

The TMR Privacy Officer reported that to date, she has not received any correspondence that would be categorised as a 'privacy complaint' under formal guidelines (i.e., a person wishing to complain or express dissatisfaction about an aspect of personal information management or violation of the IP Act). Rather, enquiries typically relate to questioning whether TMR/QRO has a 'right' to take camera images and issue infringement notices.

Based on this information, it appears that the bulk of customer complaints and enquiries are not directly related to privacy. Rather, they tend to be from customers who are aggrieved about having to pay a fine, and therefore raise objections and questions (including about privacy).

IIS acknowledges there are customers who raise genuine privacy concerns, for example how they are depicted in the camera image. While there may not be a 'satisfying' answer for them (since an offence has been adjudicated and the infringement notice must be issued), from a customer service perspective there could be ways for the MPST Unit correspondent to express empathy and reassurance in such circumstances.

The MPST Unit uses templates and inserts to help construct replies in a consistent and approved manner. IIS reviewed relevant excerpts, which includes standardised language regarding topics such as 'privacy (facial recognition)', 'Privacy in a car' and 'Person receiving notices for someone not at their address'.

IIS further understands that the following topics are included in IAP templated responses:

- Right of TMR/QRO to take camera images and administer the MPST program – Information, including links as appropriate, about the MPST program and underpinning legislative regime.
- Privacy concern about depiction in camera image – Expression of empathy and reassurance that the camera image is subject to strict controls.

As a matter of best practice, it would be worthwhile for the MPST Unit leadership team, in consultation with privacy and legal, to discuss issues and gaps in how customer complaints and enquiries are currently being handled, and to update the Correspondence Guide accordingly.

Suggestion 2 – Review Correspondence Guide to address current issues and gaps in handling customer complaints and enquiries to the MPST Unit
Collate issues and gaps in how customer complaints and enquiries to the MPST Unit are being handled. Develop additional inserts for the Correspondence Guide that address identified issues and gaps, and ensure awareness within the MPST Unit. **Who:** TMR and QRO **When:** Within 6 months

5.3 System (technical) components and data

5.3.1 Functional and technical changes to the existing IAP

IIS reviewed the provided extract of system changes to the existing IAP ('MPST - Key Changes and Potential Privacy Impact') and spoke with TMR's Business System Analyst and Technical Lead. IIS notes that the changes reviewed all had positive privacy impacts. Key areas of change are summarised in the table below.

Change Area	Comments
Audit logging	Improved audit logs were introduced to be able to review user activities. This improvement was implemented post an internal investigation

Change Area	Comments
Access restrictions	Two types of access restrictions were noted: • Introduction of a features within IAP to remove the requirement for some users to have broader access to TRAILS. • Limit access within the IAP
Picture pixelation capability	Introduced technical capability to pixelate incident images at Adjudication and QA stages. While this feature is available, QRO have determined they won't switch this functionality on for the time being

5.3.2 New IAP for QRO with external Supplier

5.3.2.1 Review of data migration strategy

The data migration strategy is not fully developed yet. However, the project team advised that the high-level approach would entail:

- Restrict functionality of current IAP to TMR's remaining responsibility in the process, namely, integration with the camera vendor and deployment validation (i.e., validation of camera image location metadata against camera schedule).
- Migrate (extract, transform, load) active incident data (including images) to new IAP.
- Switch over to new IAP.
- Retention of old system data to be decided; intention is to store indefinitely.

Based on the high-level description of the migration process, IIS suggests following privacy preserving data migration best practices.

Suggestion 3 – Consider privacy best practices for data migration

Follow best practices for data migration to new IAP:

- Ensure correctness of data transformation by performing pre- and post migration validation (e.g, wrong picture or address linked to specific incident).
- Ensure data is protected throughout its migration lifecycle (e.g., encrypted, no clear text snapshots) and effectively deleted from any temporary storage location.
- Validate 'locked-down' feature restriction and access to TMR's IAP system for both end-users and administrators.
- Consider adding an alerting mechanism if content which was designed to be inaccessible is accessed.
- Confirm retention arrangement in writing.

Who: TMR, QRO and IAP supplier

When: Before go-live of new IAP

5.3.2.2 Supplier privacy practices and policies related to IAP

In November 2022, TMR issued an Invitation to Offer titled *"Provision of Software Solution and Support enabling microservices based replacement of existing Mobile Phone Seatbelt Technology (MPST) solution"*. TMR awarded the IAP supplier the contract in October 2023.

After the initial development process, the IAP supplier will maintain and support the new IAP as a managed service and apply the relevant set of privacy and security standards policies for infrastructure, personnel, methodologies, and other resources (e.g., ISO 2700:2016, 27005:2012, Australia's ISM, Queensland Information Security Policy, Queensland Government Information Security Classification).

The development of the new solution combines developed software, technology, and API services and a new workflow software platform as the frontend. Interfaces exist to TRAILS and to a locked-down, pre-vetted and limited repository of camera images. The program leverages a modern infrastructure and development practices. Testing will be performed by the established TMR test team who have also performed the testing on the existing IAP.

QRO has reviewed and approved the architecture and continues to be consulted as part of the program. . Prior to go live, the IAP supplier will assess the solution against the Australian Signals Directorate's (ASD) ISM.

The new IAP was classified as SENSITIVE by QRO. This is because PROTECTED customers details (i.e., those relating to suppressed customers) will be handled outside of the new IAP system, leveraging existing processes.

Camera images are classified SENSITIVE as images cannot be reasonably used to identify persons in isolation.

The project team is finalising the design of the new solution. As such, IIS has not seen any detailed build documentation or operational plans. However, by reviewing available documents and by conducting interviews with relevant stakeholders, IIS has made suggestions for consideration before a 'go-live' decision – see below our discussion regarding:

- Handling of personal information and camera images
- Systematic testing for privacy controls
- System monitoring.

IIS expects that the current internal review processes by QRO and the ASD ISM mapping will result in data protection controls that sufficiently address common risk scenarios of both external and internal unauthorised actors attempting to gain access to data within the new IAP.

Handling of personal information and camera images

While protecting suppressed customer details is considered a key privacy risk by QRO, IIS heard throughout interviews that a misuse of the images by an authorised user would also have the potential to significantly impact public trust. To reiterate from above, the risk can be described as: **Unauthorised access to or misuse of TMR and QRO information by staff, contractors or third parties resulting in non-compliance with the law, harm to the customer, reputational damage to government and eroded public trust**.

IIS understands that due to an internal incident of alleged misuse of information arising from authorised logical access to the IAP, TMR improved the existing IAP's audit logging capabilities. This feature was implemented to evidence what data is accessed by users – see Section 5.2.1.1 above for further discussion on auditing function and practice.

With regards to handling the images upstream of the new IAP, IIS notes that the camera and AI provider follows a strict, purposefully designed process to minimise unnecessary retention of images or exposure of personal details as part of the human pre-adjudication process.

Privacy is best protected when built-in into a solution (i.e., privacy by design and default). A common practice used to enumerate privacy risks and treatment options during the systems development lifecycle is to leverage a privacy threat model framework. IIS has sighted a security focused, high-level threat map performed in 2021 for the existing IAP. The IAP supplier has put a generic threat model process forward.

However, IIS has not sighted an applied privacy threat model (or similar) for the new IAP that systematically analyses relevant privacy risks. IIS expects that such analysis would result in recommending privacy controls to stay within risk appetite and would include all systems used for the solution.

Example controls for a specific misuse risk scenario may include:

Short-hand scenario description	Control examples
Misuse of access to camera images by authorised end users.	• Rate limit access of end user to data elements • Record “reason for access” as a deterrent control and as a data point for automated, algorithmic reviews. To reduce the end user burden, consider when “reason for access” is required (e.g., when data is being accessed via search instead of an assigned queue) • Create real-time review alerts (and possibly block access) for when thresholds are reached. Allow a management user role to adjust and/or reset rate thresholds • Create real-time review alerts (and possibly block access) for conditions where there might be an increased likelihood of misuse of information (e.g., staff surname or address matches customer’s address of infringement) • Schedule automated, regular end user access reporting for management review • Implement granular access control to enforce principle of least privilege.

Unauthorised access to camera images by administrative accounts and/or third parties.	• Implement granular access control to enforce the principle of least privilege for access to camera images by administrative and third-party staff:
	  ○ require additional approval and business justification to elevate privilege to access images.
	  ○ use separate high privileged administrative account and review use
	• Request regular access reports with access statistics from third parties
	• Schedule automated, regular administrative or third-party access reporting for QRO to review.

IIS recommends that TMR, QRO and the relevant future party contracted to maintain the system (once the IAP supplier has built the system) collaborate in performing a privacy threat analysis for the new IAP.

Recommendation 8 – Perform a privacy threat analysis and strengthen mechanisms to prevent, detect and respond to unauthorised access to and misuse of camera images

Perform privacy threat analysis by modelling scenarios involving unauthorised access to, or misuse of, camera images for the new IAP.

Implement appropriate technical and administrative controls to reduce risks identified in the privacy threat analysis.

Who: TMR, QRO and relevant contracted party

When: Within 6 months

IIS understands that the new solution design proposes to persistently store encrypted address and name of offenders with vehicle details for infringement notices in the new workflow software platform and to retain that data indefinitely. All other information (e.g. any attached statutory declarations, images) are retrieved at runtime via API from the database backend. IIS heard that this is the only personal information to be retained with the new workflow software platform and the data will be protected in the underlying platform by encryption. However, from a data minimisation approach, this is a suboptimal solution.

Suggestion 4 – Consider avoid storing personal details in the new IAP

Consider re-exploring the possibility of retrieving PI on demand from the database backend to avoid storing a copy of the address and name of offenders in the new workflow software platform. If deemed not feasible, record rationale, risk and mitigation.

Who: TMR, QRO and IAP supplier

When: Before go-live of new IAP

Systematic testing for privacy controls

TMR has a well-established testing team that has performed the testing for the existing IAP. IIS has sighted internal documentation and considers that there are further areas for testers to validate. IIS heard that the team checks for input validation issues when new data fields are being introduced. Further, IIS notes that penetration testing is planned before the new IAP 'go-live'.

IIS has not sighted or heard about a systematic test plan for privacy controls and privacy requirements or regular attempts (other than input validation on new data fields) to "break the system" or ways in which privacy may be violated by a misuse or abuse of the software's functionality.

Designing and testing software to meet privacy and security requirements and to mitigate privacy and security risks are fundamental phases in the software development lifecycle. Given the risks of harm to the data subject and reputational damage to government, we consider the current practices are insufficient and suggest formalising the approach to privacy threat modelling (e.g., LINDDUN privacy threat modelling framework) and testing.

Suggestion 5 – Formalise privacy testing process

Update test documentation to formalise systematic testing of privacy concerns and features.

Consider input from threat models to create automated and manual testing procedures (e.g., ensure privacy related access audit logs are correctly generated and logs are free from personal information). Include all components of the system under review, including the new workflow software platform's customised components and components that may be affected by configuration issues.

Who: TMR and QRO

When: Before go-live of new IAP

System monitoring

IIS understands that the operating model for system monitoring has not yet been defined. Monitoring the system components for anomalies and signs of data breach is key to operationalising privacy protection (refer to data misuse recommendations above).

IIS considers this particularly important for complex solutions consisting of multiple components and shared responsibilities . An effective operating model should consider the synergy of available data to detect and respond to security and privacy events and should clarify responsibilities in monitoring and responding to events.

Suggestion 6 – Confirm the monitoring approach for the operating model for the new IAP

Ensure the operating model to monitor the new IAP is in place before 'go-live'. This includes:

- Sending all relevant monitoring data (including system access log) to a log system of choice (e.g., SIEM) monitored by a Security or System Operating Centre (SOC)
- Agreeing on initial alert thresholds and implementing an on-going review to test and adjust the monitoring process
- Clarifying roles and responsibilities between the managed service provider and QRO's in-house SOC.

Who: TMR and QRO

When: Before go-live of new IAP

5.3.3 Changes to camera scheduling

IIS was asked to consider the current camera scheduling system and changes since the previous PIA, as well as plans for the new camera scheduling solution.

IIS spoke with the Principal Advisor in charge of scheduling cameras at TMR. We understand that the cameras are manually randomised across various sites for deploying the camera. The specific sites are determined by operational feasibility and crash statistics.

IIS understands that the only change to the existing process since the previous PIA is that additional sites were added in 2022 and have become part of the camera deployment rotation.

The previous PIA raised a potential concern with community perception of program bias, for example if the MPST program consistently places cameras in areas experiencing high crime rates, low employment rates, proportionally high representation of certain ethnic group(s) or other community characteristics. Based on TMR's experience since then and the absence of specific community concerns around this issue, it appears that such risks have not eventuated.

Furthermore, IIS considers that neither the current methods for site selection (based on operational feasibility and crash statistics), nor camera deployment (based on a 'manual randomisation' approach), contribute to the risk of actual bias or specific targeting of communities.

Nevertheless, there is room for improvement in camera scheduling. TMR acknowledged that the current method of manually randomising the deployment of cameras does not meet the road safety standard for true randomisation. TMR informed IIS that the plan was to have an automated scheduling solution, however this was unable to be achieved for go-live of the MPST program.

IIS understands that TMR is going to market for an automated scheduling solution, with the tender to close by end of January 2024 and the potential solution to be implemented in the second half of 2024. TMR informed IIS that in addition to better randomisation, it is intended that the solution will allow for configurable business rules for scheduling.

IIS supports the introduction of an automated scheduling solution as a matter of best practice. We have not identified any additional privacy or social licence issues with camera scheduling at this stage.

5.4 Other issues

5.4.1 Media attention and public expectations

The MPST program in Queensland, and similar programs in other jurisdictions, have received media attention due to individuals reporting that the roadside camera has captured them in an embarrassing or indecent way. For example:

- A couple on the Gold Coast complained to the media and authorities after receiving a seatbelt infringement notice that included a photo of the wife with her underwear visible, while resting her feet on the dashboard of the ute.[5]
- A woman in NSW complained to the media and authorities after receiving a photo accompanying her fine in the mail that shows her 'upskirt' with her underwear visible.[6]

Queensland's MPST program has also received general media coverage and attracted commentary from a civil liberties advocate.[7]

IIS considers that this is a tricky situation because, for QRO to properly administer the MPST program, the infringement notice (with supporting images) must be issued where there is a mobile phone or seatbelt offence, regardless of what else is in the photo. This could cause embarrassment to the individual and lead them to complain to the MPST Unit (see further discussion at Section 5.2.4) and/or to the media. Therefore, it is inevitable that such cases will attract media attention, depending on the actions of individuals.

The question for TMR and QRO is whether this is an acceptable risk (given the sporadic nature of media attention and no evidence of systemic loss of public confidence), or whether more could and should be done to manage it.

[5] See, e.g., news.com.au, 'Couple demand apology after traffic camera takes photo up wife's skirt' (24 January 2023) <https://www.news.com.au/technology/motoring/on-the-road/couple-demand-apology-after-traffic-camera-takes-photo-up-wifes-skirt/news-story/4c812442f8b23fe0300c97548591ebc2>.

[6] See, e.g., news.com.au, ''Shock & distress': upskirt photo prompts camera review' (12 March 2023) <https://www.news.com.au/national/nsw-act/shock-distress-upskirt-photo-prompts-camera-review/news-story/6ffe21221bb68d47e7e9d92e3a0c79f1>.

[7] See ABC News, 'Queensland phone, seatbelt cameras could face review amid 'sexual privacy rights' concerns' () <https://www.abc.net.au/news/2023-03-17/queensland-phone-seatbelt-cameras-review-sexual-privacy-rights/102110194>.

TMR has built the capability to pixelate images into the existing IAP. This would provide the technical ability for explicit or sensitive parts of the image to be 'blurred out'. The feature has not yet been made available to MPST Unit staff. IIS understands that, at present, MPST Unit executives have made a policy decision not to use this feature because it may raise questions about the integrity of images and undermine confidence in the MPST program. They want to ensure public confidence in image integrity – that is, images presented to customers are not modified and are an accurate depiction of the originally captured image. Furthermore, the pixelation of the images does not mitigate public concerns that the sensitive content was captured in the first place.

IIS consulted with OIC as part of the PIA process and raised this issue with the Privacy Commissioner and Acting Assistant Privacy Commissioner. Key points from the discussion include:

- While people using public roads are subject to road laws, it would be wrong to dismiss their expectation of privacy when driving in their own vehicle – there is a qualitative difference between noticing someone driving past at high speed and taking a high-quality still image of that person
- The privacy risk is heightened because the registered operator of the vehicle (who receives the infringement notice at the first instance) may see an embarrassing image of the passenger who has committed an offence
- There should be a balance between carrying out the fine administration function and minimising privacy intrusion
    - It would be beneficial as a matter of accountability and transparency to go through a documented consideration of the options (regardless of the conclusion reached)
- The blurring of a particular part of the image does not affect its usefulness in demonstrating there was an offence
    - Furthermore, concerns about image integrity could be addressed by messaging that the blurring has been done to protect privacy; this is a defensible reason that most people would understand
- As a matter of internal management, the MPST Unit should use all feasible controls – including training and awareness – to protect the images.

Based on the above, IIS encourages the MPST Unit to revisit its decision to not use the image pixelation feature. As noted by the OIC, public concerns about image integrity can be addressed through communications – for example, in the infringement notice, relevant websites and information pages – that explain why a particular part of the image has been blurred (to preserve privacy) and that the original file is available for review on request.

Regardless of what the MPST Unit decides, it should document the reasons for its decision.

Suggestion 7 – Revisit and document decision as to whether the image pixelation feature should be used by the MPST Unit

Revisit decision as to whether the image pixelation feature should be used by the MPST Unit. Consider pros and cons, and whether and how concerns around image integrity could be managed (e.g., through communications).

Document the decision-making process.

Who: QRO

When: Within 6 months

5.5 Conclusion

IIS has not identified any show-stopping privacy issues for the MPST program, and we consider that its business as usual (BAU) operations are largely compliant with the IPPs.

The MPST program has been operating smoothly in BAU. The changes that have occurred (e.g., MOG changes, physical move to a new office) and the changes that are still in train (e.g., design and development of a new IAP) present opportunities for the MPST Unit to uplift its privacy practices, procedures and systems.

With several important issues to manage as the new IAP is developed and rolled out, IIS considers the residual privacy risk is **medium**.

Privacy risks are likely to be within manageable levels, subject to the recommendations we have made in with respect to:

- Further access controls and audit practices
- Strengthened retention and deletion practices for images and personal information
- Better documentation of policies, standards and procedures, with accompanying training
- Further privacy risk due diligence for the new IAP.

IIS thanks TMR, QRO and all PIA stakeholders for their time and cooperation during this PIA. We are available to discuss the report with TMR and any other stakeholders.

6. Appendix A – Scope and methodology

A.1 Scope

TMR and QRO engaged IIS to:

- Address the following in scope matters:
  - Review changes to the MPST adjudication process since the original PIA;
  - Change with MPST Unit moving to QRO;
  - Changes with scheduling of cameras;
  - Functional and technical changes to the existing IAP that have occurred;
  - New IAP for QRO;
  - Media attention that has arisen and may arise;
  - Assess the design of personal information handling practices;
  - Confirm privacy risks reported in previous PIA have been addressed; and
  - Assess design of the privacy complaints management process within the MPST Adjudication Team.
- Identify the privacy and security risks associated with the above and provide recommendations to mitigate such risks.

A.2 Methodology

IIS took the following steps to carry out the PIA:

- *Planning* with TMR to confirm the approach and deliverable.
- *Gathering information* by reading documents and meeting with staff from TMR, and with other stakeholders.
- *Analysing* the information against privacy obligations and taking account of possible broader privacy issues, regulator guidance, and privacy best practice.
- *Identifying privacy risks* and developing ways to mitigate those risks.
- *Developing a set of preliminary findings and recommendation* for TMR's comments.
- *Drafting PIA report* and providing this to TMR for comment on matters of fact only.
- *Addressing feedback*, *finalising* the draft of the first report and *providing final report* to TMR.

7. Appendix B – Assessment against the IPPs

The following table sets out IIS's high-level assessment of the MPST Program against the IPPs.

IIS also notes that where our assessment has not identified specific issues for this PIA, that is not meant to indicate there is no privacy work to be done. IIS anticipates that usual privacy compliance and monitoring would occur.

Summary of privacy principle	High level assessment against IPPs
IPP 1-3 Collection An agency may request personal information from an individual or from a third party provided the following criteria are met: • The agency must only ask for the specific personal information required to fulfil the lawful purpose that is directly related to the function of the agency • If the information is collected directly from an individual, the agency must tell the individual what the information is going to be used for before, at, or as soon as practicable after the information is collected • The agency must not collect information by unlawful or unfair means • The agency must take reasonable steps to ensure that personal information is relevant to the purpose for which it is collected, complete and up to date, and does not unreasonably intrude into the personal affairs of the individual.	The MPST program collects personal information in the following ways: • Camera images and metadata, from TMR (originally collected by the camera and AI provider) • Registration and licensing information from TRAILS and TICA • Information from customers as part of dealing with enquiries and disputes about infringement notices. There have been no changes in collection since the first PIA. IIS considers that the collection continues to be lawful and necessary for the MPST Unit's functions and activities. There may be improvements in how QRO could better notify individuals about collection. However, this should be better considered as part of broader privacy activities and is out of scope for this PIA.
IPP 4 – Storage and security Agencies must ensure that documents containing personal information are protected from: loss; unauthorised access, use, modification or disclosure; and any other misuse.	Given the risk context of the MPST Unit and the quality and quantity of potentially sensitive information that it handles, IIS considers that the kinds of protections in place are reasonable in the circumstances, but can be further strengthened. See the discussion in the findings sections above – IPP 4 is one of the main considerations for this PIA.

Summary of privacy principle	High level assessment against IPPs
The protection must include security safeguards that are reasonable in the circumstances.	
IPP 5-7 – Access and amendment IPP 5 requires agencies to disclose to the public the general types of information they hold, for what particular purpose, and how the information is proposed to be used. IPP 6 sets out how an individual may request access to their personal information. IPP 7 relates to the amendment of personal information held by agencies, and requires an agency to take all reasonable steps to assure the quality and accuracy of personal information prior to using it.	TMR provides details about the handling of MPST information in its publicly available Information Privacy Plan. Individuals can request access and amendment of their information under existing processes. The MPST Unit would refer customers back to TMR if it receives correspondence regarding access to or amendment of their customer details. No further issues identified.
IPP 8-10 – Use IPP 8 – Before an agency can use personal information, it must take reasonable steps to ensure that the information is accurate, complete and up to date. IPP 9 – When an agency proposes to use a document containing personal information for a particular purpose, the agency must only use those parts of the personal information which are directly relevant to fulfilling that particular purpose. IPP 10 – Personal information must not be used for a purpose other than the particular purpose for which it was obtained, unless certain exceptions apply.	The MPST Unit has quality assurance arrangements in place (including multiple levels of human review) to ensure that its adjudication decisions are accurate. Apart from this, it relies on the information provided by TMR. The governing MOUs between TMR and SPER/QRO have provisions for maintaining data quality and integrity. Along with IPP 4, IPPs 9 and 10 are the main considerations for the PIA, in terms of ensuring that the MPST Unit does not use more personal information than is required, and that it protects against misuses. See the discussion in the findings sections above.
IPP 11 – Disclosure Personal information must not be disclosed to a third party, unless certain exceptions apply.	In the context of the MPST program, personal information may be disclosed to external parties in the following circumstances:

Summary of privacy principle	High level assessment against IPPs
	• Law enforcement or other authorities, for law enforcement purposes, in relation to DFV situation, etc. • Back to individuals as part of RTI requests • MP's office, in response to ministerial requests (with the individual's implied consent) • Media organisations (with the individual's consent). IIS considers that such disclosures would meet at least one of the exceptions in IPP 11. No further issues identified. IIS reiterates the importance of measures to reduce the risk of unauthorised access, which could also lead to a breach of IPP 11. See discussion in the findings sections above.
Section 33 – Overseas transfer Agencies must not transfer personal information overseas unless there is consent, legal requirement or public health or safety reasons.	No personal information is held or transferred overseas as part of the MPST program. All information involved is stored in systems hosted in Australia.

INFORMATION INTEGRITY SOLUTIONS PTY LTD
PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438
F: +61 2 9319 5754
E: contact@iispartners.com
www.iispartners.com

ABN 78 107 611 898

ACN 107 611 898

IIS Partners
INFORMATION INTEGRITY SOLUTIONS